Docket No.: 4502-1085 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of :

Christopher James MASSAM et al :

U.S. Patent Application No. 10/540,328 :

For: NETWORK DEVICE CONFIGURATION

AFFIDAVIT OF SIMON MATHEW GAMBLE

I, Simon Mathew Gamble, Company Director of Auckland, swear:

1. I am the Business Development Director of Mako Networks, which is the trading name of YellowTuna Networks Ltd, which is the operating subsidiary of YellowTuna Holdings Ltd the assignee of the inventors of the present application.

2. In this affidavit I will refer to the invention as "the Mako modem" or the "Mako VPN" or the "Mako Management System".

3. I have read the PCT specification filed on behalf of YellowTuna Holdings Limited namely PCT/NZ2003/000265 published as WO 2004/059508, which specification is the basis for this US national phase application.

4. I am not one of the inventors of the invention described and claimed in the present US patent application. The inventors Christopher James MASSAM and Dennis Warren MONKS are personally known to me, and I work with them.

5. I have also read and considered the cited patent by Hughes namely US Patent 6,854,009. I will discuss that towards the end of my affidavit. In the meantime I need to set the background of this invention, and to explain the Mako system which is the subject of the present US patent application.

6. The major difference between the network device of the present invention described and claimed in the method of this US patent application and comparable traditional devices, is that the Mako network device does not carry on it any of the configuration data required for it to perform its tasks prior to being started up. It may contain a default ISP connectivity configuration in order that it can connect to the internet automatically. Alternatively, it may receive its basic internet connectivity configuration via a supplied USB key or SMS message. This provides an additional layer of security to the network device. Because the end-user's private configuration data is not domiciled on the device it cannot be accessed and/or modified to allow unwanted access to the device or the network it is protecting. The configuration data is communicated to the network device once it has been connected to an ADSL circuit and powered up, by our verification authority.

7. In designing our Mako modem (the network device of the claims) our mission statement was "You should be able to plug it in and it goes.". This has been achieved by the design of our network devices, and the operation of our system.

8. Since I graduated from university I have always worked in the IT industry in New Zealand. Beginning in 1994 with Datamatic, at the time the NZ representative for Cisco, Novel and many other hardware and software brands. Most of my work at Datamatic was with their training centre; Datacollege. In 1996 my manager at Datamatic was head-hunted to go to Telecom's newly formed ISP; Xtra. I followed shortly after and began working on the help desk as a tier three engineer.

9. I soon migrated to the IT department as a Unix Systems Administrator. It was working in this role that I was exposed to the real workings of the internet in a live environment. After a couple of years as a Systems Administrator I moved into the specialised Systems Security team responsible for the security of the Xtra network. I remained in this position until my resignation in 2000.

10. When I first started at Xtra in 1996, dial-up modems were used by the vast majority of home and business users to connect to the internet. Only very large organisations could afford high speed, always on connections. But in 1998 Telecom introduced a new technology called ADSL (Asynchronous Digital Subscriber Line) to the New Zealand market. ADSL used the existing copper phone cable infrastructure to provide an affordable always-on broadband internet connection.

11. Countries like the USA had had access to cheap broadband for a number of years which ran over their existing cable TV infrastructure. New Zealand (and most other countries) had no such network to carry high speed data until the introduction of ADSL.

12. The connection of DSL modems to the internet are explained in various documents on web sites, of which the following are useful examples:

http://www.kitz.co.uk/adsl/equip2.htm for a complex one, http://www.dslreports.com/information/kb/DSL-1/pictures for a simpler one, http://cc.1asphost.com/geowcloo/adsl/DesignImplementation.htm for something more easily understandable.

13. ADSL brought broadband to within reach of anybody and enabled smaller businesses to begin to use the internet as a real business tool.

14. But it also brought with it a lot of problems for both the end user and the ISP. The problems weren't exclusive to ADSL - but rather problems related to the mass commercialisation of broadband. Problems of how to deploy, support and manage broadband. The fact that the technology wasn't simple to configure and set up meant that end users couldn't easily get the most out of their connection without costly technical assistance.

15. An "always on" connection to the internet brought with it a new raft of security concerns that many businesses weren't aware of until too late. The convenience of high speed internet at work meant many hours of staff productivity was being lost also.

16. Configuring, deploying, and connecting the new ADSL modems and routers was a very hands-on affair. And customers were not prepared to pay the full cost of onsite deployment. In the end, Telecom wore that cost one way or another as if the customer elected to self-install, they invariably spent hours on the phone to the help desk.

17. Once the broadband connection was up and running, it was never quite as easy to get things working as it appeared in the marketing literature. Firewall pinholes needed to be opened in order to allow email and other services to work. Establishing VPNs to be able to work from home or share inter-office accounting systems was a costly exercise for the customer and a PR nightmare for Telecom.

18. It was clear that the new broadband technology could bring significant benefits to business but it needed to be easier to control, configure, and understand for the end user. It also needed to be much cheaper to deploy and support for the ISPs.

19. I have also annexed hereto marked with the letters "SMG-1" a true copy of a brochure entitled "The Mako System" which I have downloaded from my company's web site. This provides an overview of the system, and some examples of information that a customer can obtain from our web site.

20. The importance of these documents is that they show that the invention here is a "system" which combines the appliance (for simplicity I will call it a router) with a hosted central management platform, so that the two things work together to provide a complete network connectivity and management solution designed

specifically for small to medium sized enterprises. The entire configuration of the Mako appliance (called the "network device" in the claims of the present application), takes place over authenticated HTTPS on the central management platform. There is no need for a technician to go to the customer's site to install a configuration on the appliance itself, in fact this is not possible because of the design of the appliance. In our brochures and drawings we often use the abbreviation "CPE" to refer to the network device. "CPE" is the standard abbreviation for "Customer Premises Equipment" which distinguishes it from equipment at the telephone exchange or from other companies outside the customer's premises.

21. Because the system itself is controlled by the management server, called the "verification authority" in the claims of the present application, it is possible for the verification authority to manage a very large number of routers, to collect traffic information from them, to update their configurations as and when needed, and more importantly in the case of the present application to enable two different routers without static IP addresses, without the need for technicians to be on site to set the VPN, because the verification authority stores the current public IP address of each router, and enables each of the routers to contact the verification authority, find out the IP address of the other router, and quickly and easily create a VPN between the two routers each of which would otherwise not know the others address. I will explain the problem setting up a VPN without this invention in the following paragraphs and then contrast it with the operation of this invention.

22. Prior to this invention, when we were building the Linux-based firewalls, we would typically place them behind an ADSL modem/router device. We'd have to leave management pinholes open on the firewall to allow connections from our static IP address to be able to administer the customer's configuration settings. All the modems/routers needed to be manually set up beforehand and deployed manually with a site visit. If a customer called with a problem, we'd have to look up on a table to find their static IP address in order to begin troubleshooting or to change the configuration.

23. If a modem lost its connection to the internet, often it would not be able to recover without a manual reboot.

24. Modems are by their nature a relatively simple device designed to enable digital signals to travel over an analogue carrier.

25. Modems need to be configured so that they connect to whatever device that answers at the end of the line in a manner that is expected and compatible. More often than not, there is a unique identifier such as a user name and password combination that requires each modem to be individually configured. Nearly every ISP in the world uses different settings even if they share the same

technology (such as ADSL) with other ISPs. This all adds up to each modem going out to each end user needs to be individually configured.

26. Once the modem is configured and deployed to the customer premise, some form of feedback loop is required to advise the installer as to the status of the connection. Failure to connect can be caused by many factors; some to do with the modem, others to do with the cabling or Telco/ISP equipment. Sending an engineer out to each and every deployment for a service that may only reap the ISP $39 per month is not very cost effective.

27. Some modems include a management interface accessible from the LAN side and which can be opened up to the WAN side via firewall pinholes. Being able to access this centrally requires a fixed IP address and offers up to the hacker community an opportunity to break into a customer's network.

28. Monitoring the performance of traditional vendor's modems is often either impossible due to a lack of facility/function or more commonly requires the installation of an SNMP monitoring server. SNMP is an acronym for Simple Network Management Protocol. Some third party vendor's modems include support for SNMP. This functionality lets a monitoring server log into the modem and collect pre-defined stats. The monitoring server needs to be built and maintained and needs to know the IP address of the monitored device.

29. The Mako System was born because three former employees at Telecom Xtra could see the benefits of broadband waiting to be exploited but also the pain to the ISP and the customer.

30. We started out building Linux-based firewalls for small businesses. These firewalls would protect the businesses from many dangers of the internet and could be easily remotely controlled by us. The business was successful but also not easily scalable as it was very hands on. We needed to build an automated, easily scalable solution - Mako.

31. I have annexed hereto marked with the letters "SMG-2" a true copy of the "Mako Networks system summary" taken from my company's web site. In the drawings shown on the first page the Mako command servers correspond to the "verification authority" described and claimed in the present application. The reference in this document to "patented proprietary software "refers to the family of patent applications corresponding to this US application, for which patents have been granted in New Zealand and in other countries.

32. There are many types of VPN ("virtual private network"). One of the most secure and useful types of VPN is an IPsec VPN (where IPSec is an abbreviation of "IP Security"). IPsec VPNs link an entire network to another network via an encrypted tunnel over the internet. They are described in many publications, one example of which is The National Institute of Standards Publication 800-77 which

can be found at http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf. Largely because of their high level of security, they are notoriously difficult to set up properly.

33. IPsec VPNs are very useful as they run at the Internet Layer of communication. This means that any application that communicates using TCP/IP can make use of the IPsec VPN and does not need to be built to know about IPsec unlike many other types of VPN.

34. An IPsec VPN tunnel requires at least one end of the tunnel to have a static IP address. It also needs some sort of key or certificate to be configured at each end as well as a number of other configuration options. Traditional vendor's devices are usually configured manually and then taken to the customer's premises where the VPN is brought up. This often requires an engineer at each site communicating with each other by telephone to confirm the tunnel is active and to make necessary modifications to the configuration.

35. Creating a site to site IPsec tunnel using the Mako system requires three mouse clicks on the secure management website. Static IP addresses are not required and no specialised knowledge is necessary. Mako IPsec tunnels can be established at any time and torn down at any time via the secure management website. It is the communication method between appliance and management node that enables this and many other functions of the Mako system.

36. I have annexed hereto marked with the letters "SMG-3" a copy of a drawing explaining the Mako modem start up routine and the storage of the allocated IP address of the modem at the configuration server so that a VPN can be created between devices that do not have static IP addresses.

37. When the modem wakes up it tries to create or find an internet connection. In the simplest case it has DSL connection parameters for a Mako DSL connection, and it uses these at 307.

38. At 310 we talk to the verification server and at 314 we get the client Config data from the Config service. The system does not care if the IP address is permanent or not – cpe is treated the same regardless. The modem overlays its default DSL Config and restarts the DSL service using the client Config – which may be for a different ISP than Mako's one.

39. It contacts the Verification Authority again to confirm it is on line and to allow the Config service to extract its internet address where this is a temporary one from the ISP. Then it settles down to being a modem and regularly delivers its traffic logs to the admin service for traffic information etc.

40. Whenever a VPN is required between two or more of the network devices, it is easier to set up by the user creating a VPN via the https web site. This web site

allows control of the verification authority which stores the various IP addresses for the different network devices, and the verification authority then sends an instruction to the Mako modem to create a VPN to a given address. As explained above it does not matter if the IP address is permanent or not, that address is stored by the verification authority, and can then be sent to the modem which initiates the VPN connection to the other network devices IP address.

41. Without the Mako central management system, there is no way to establish an IPsec tunnel between two devices without knowing the internet address of at least one of the end points. There was no way prior to Mako to setup and establish an IPsec tunnel between two end points of unknown address. It is the Mako system and communication method that enables this functionality.

42. Because the Mako appliances communicate every two minutes with the command servers, the system is kept informed of the appliances' current public IP address. Unlike other management platforms, because it is the appliances that initiate communication with the command servers, the command servers do not need to be pre-configured to know the addresses of the appliances. I have prepared an additional drawing to show the VPN connection between two network devices. These are identified as CPEA and CPEB in my drawing. I have annexed a copy of this drawing as exhibit "SMG-4". In the drawing CPE stands for "Customers Premises Equipment" and corresponds to the network device of the present claim. The command server corresponds to the verification authority which stores the allocated internet address of each of the network devices A and B. The key feature here is that the verification authority (command server) stores the public IP address of each of the network devices, and is thus able to send a command to network device A telling it to connect to network device B, and vice versa. Thus it does not matter if the network device A or B looses power, and then is reconfigured and possibly given a new IP address, because whenever it is given a new IP address that is stored at the verification authority, and the customer can then connect to the verification authority request that a VPN be connected between network devices A and B, and the verification authority can then issue that command to one or other of the network devices telling them to connect to the other device at the network address stored by the verification authority.

43. If an administrator logs into the command system and chooses to connect two Mako protected networks via an IPsec tunnel, the system already has the required information; public IP addresses, private LAN schemas and can instruct each relevant appliance to initiate a connection to the other when they next check in during their two minute window.

44. Mako to Mako IPsec VPN tunnels can thus be established without the need for the user to know any networking information and without the need for static IP addresses. I have annexed hereto marked with the letters "SMG-5" a schematic showing the connection between the two network devices listed as ASDL

modems connected via a DSLAM to the internet, and thus to the verification authority and configuration server.

45. Whenever a Mako router is connected to the internet, it will have a public IP address. In the case of Mako routers connecting using ADSL or 3G technology, that IP address is assigned by the ISP (typically at the authentication phase). A large percentage of these ISPs assign a random IP address from their pool of IP addresses and this IP address can and does change from time to time (how long between changes depends on each individual ISP).

46. With traditional vendor's routers, creating an IPSec tunnel requires at least one end of the tunnel to have a static IP address. With Mako this is not necessary.

47. I have read the cited patent US 6,854,009. My understanding of Hughes is that it describes the automatic downloading and use of a computer operating system and applications. This OS and apps can be essentially rented from a provider and then removed or disabled from the appliance when use is no longer needed or if the customer's credit dries up. Hughes assumes a connection to the internet is already present and does not describe how to establish that connection to the internet. Hughes does state that if the appliance cannot communicate with its required server, it can dial out over PSTN (assume to a BBS or some preconfigured internet dialup provider) and attempt to gain access to the server that way. I cannot find anything in Hughes about setting up and maintaining a VPN.

48. Hughes does not give any information on the design and operation of modems. Rather it simply states that the appliance can connect to one via Ethernet and use the high speed connection provided by it.

49. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that wilful false statements and the like so made are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code and that such wilful false statements may jeopardize the validity of the application or any patent issued thereon.

Simon Mathew Gamble

Sworn at Auckland this 17th day of July, 2009.)
)
Before me:)
)
)

A Solicitor of the High Court of New Zealand

James William PIPER

The Mako System

MANAGED NETWORKING AND SECURITY

Overview

Mako offers clients a centrally managed, turnkey solution for networking and security. Utilising a combination of modem, VPN router, firewall and Mako Central Management Systems the Mako provides anytime/anywhere access and real time management, reporting and proactive security in one easy to use, easy to deploy solution.

VPN (Virtual Private Network)

Mako allows you to securely connect remote users and multiple locations simply and cost effectively using VPNs. With Mako the setup time is minimal needing just three mouse clicks via the secure Central Management System. No static IP addresses are required. Remote access allows you to work securely from home, across offices from your desk or from any internet connection whilst travelling.*

24 Hour Remote Control/Diagnostics

Mako utilises the Mako Central Management System for you or your designated IT Professional to have 24 hour secure remote control over your connections to the Internet. Via the Mako website, you can modify firewall rules, create and disable VPNs, check usage patterns change your networks IP addressing and even run diagnostics.**

Complete Security

Your Mako is managed by the Mako Central Management System. It ensures that your networks are always fully protected. The protection software is automatically updated and all intrusion attempts are safely dismissed. Your Mako incorporates a stateful inspection firewall. This means that all traffic entering and leaving your networks is analysed comprehensively to ensure complete network integrity.

Connection Method

You have a choice of using ADSL, Ethernet or 3G to connect your networks to the Internet at high speed. Mako also incorporates a fully featured TCP/IP router, acting as the gateway to the Internet for all computers on your networks in each of your offices.

Tracking/Reporting

Your Mako gathers traffic and website information and sends it securely to the Mako Central Management System. The system interprets it and stores it for monthly reporting or on-line viewing. Reports are automatically delivered with detailed traffic, security, user, mail and website information. Simply log on to the Mako website to drill down on the details to identify inappropriate staff behaviour and take action to ban access to high use websites. The Mako even recommends the best broadband plan for you based on the usage from the previous month.

Email Sanitisation

The MakoMail option provides advanced virus and spam elimination for all your mail users. It also provides content filtering to ensure mail is clear of unwanted material.

Firewall

Central to the security of your networks is the type of firewall you use. Mako utilises a stateful inspection firewall. A stateful inspection firewall does not just examine packets of information, instead it makes decisions based upon information derived from all communication layers and from other applications. This type of firewall provides true enterprise level protection. Working with the Mako Central Management System, you have full control over all traffic entering and leaving your networks.

QoS (Quality of Service)

Mako ensures the best performance possible for your broadband connection. Internet Telephony (VoIP) upstream prioritisation assists in clarity and latency during calls. All other traffic can also be prioritised from the Central Management System.

*Third party VPN client software may be required.
** Some Advanced Features not available on all models. Some features carry an additional cost

Mako NETWORKS ®

This is the exhibit marked "SMG-1"
referred to in the affidavit of
Simon Mathew Gamble
sworn before me this 17/07/2009

Solicitor of the High Court of New Zealand

The Mako System

MANAGED NETWORKING AND SECURITY

Mako Benefits

Mako allows the quick linking of existing offices and easy set up of new offices with one, cost effective, easy to use system. It gives complete control and visibility anywhere/anytime, is managed remotely and updated automatically.

- Rapid deployment of new offices or sites
- Easy connection and management of multiple sites
- Access to your network 24/7 remotely and securely from any internet connection
- Summarised easy to understand monthly reports emailed to you
- Detailed reporting available online, anytime/anywhere
- Lower business overheads through the mitigation of unforeseen costs e.g. reduction of Corporate risk by limiting employee access to potentially litigious content and data cap management on internet plans
- Complete control and visibility of your networks
- Increase staff productivity by reducing internet procrastination
- Enterprise level security protecting against worms, spam, viruses and malware
- No manual security or feature updates – it's all automatic
- Lower cost of network management and maintenance and increase network uptime with the comprehensive diagnostic and management tool
- Lower cost network with all the benefits of a private higher cost solution

Central Management

The Mako control service utilises a Central Management System that offers 24hour remote control over the company's internet connections. Through this service users can modify security rules, create or disable VPNs, run diagnostics and track internet usage.

The Content Filtering feature provides additional control to the network administrator and allows them to define the content or websites that can be accessed by the network.

The Central Management System securely stores traffic and website information and provides companies with a detailed monthly report on traffic, security, user, mail and website visit information. The reports are easy to understand and include actual websites visited by computer which allow you to see instantly which users are using the internet and for what purpose.

Automatically generated warnings are sent if you approach your broadband usage limit and an automatic pause in access is created when the personalised maximum access is reached.

Features:

- Hosted Central Management Servers
- Access via internet 24/7
- Content Filtering
- Bill Shock Protection
- Remote Provisioning and Configuration
- Automatic Alerts
- Detailed Usage Reporting
- Diagnostics

Mako

NETWORKS ®

The Mako System

MANAGED NETWORKING AND SECURITY

VPN - Link Your Sites

Linking multiple sites is extremely cost effective and easy using Mako because it operates in conjunction with any public broadband ISP service. A Mako at each site not only gives you total network security, it also provides a secure, high speed pipe between branches nationwide or worldwide.

Sharing company files, working from home, or controlling your business from the other side of the world is easy and affordable with Mako.

With Mako you have a choice of ADSL, Ethernet or 3G solutions to connect your network. The System incorporates a fully featured TCP/IP router which acts as the gateway to the Internet for all computers on your networks.

With Mako traffic can be prioritised via the Central Management System and Internet Telephony VoIP upstream prioritisation assists in clarity and latency during calls. This means you get the best performance from your broadband connection.

Features:

- IP / Internet Based Transport
- Low cost Broadband connections
- Encrypted VPN links
- No Static IP address
- Supports Dynamic DNS
- Remote Access built in
- Choice of connection method

Network Security

With Mako you can securely connect remote users using VPNs. The Central Management System, Email Sanitisation and Firewall all ensure that your networks are fully protected. Security and other Mako features are updated remotely so you always have up to date security measures in place.

Mako looks for virus, trojan and botnet behaviours as well as code and blocks intrusions before they get to your network. Should a computer on your network become infected the System will identify and quarantine the infected device automatically and alert your administrator via email.

The System provides affordable enterprise level security with 24/7 monitoring and security ensuring peace of mind for business owners.

Features:

- Stateful Firewall
- Deep Packet Inspection
- Intrusion Detection System
- Worm, Spam and Virus Elimination
- QoS for VoIP
- Single or Dual Ethernet
- Content filtering
- Completely remote controlled
- Automatically Updated

Mako
NETWORKS ®

The Mako System

MANAGED NETWORKING AND SECURITY

Visibility and Control of Your Network

A complete network management tool with detailed usage reporting.

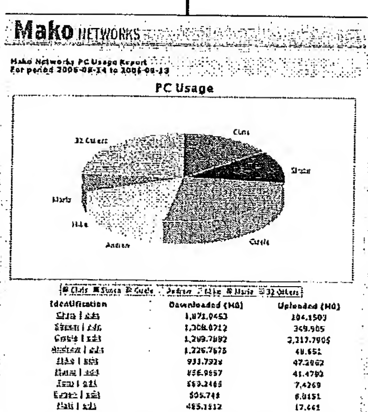
Key Features of Mako Reporting:

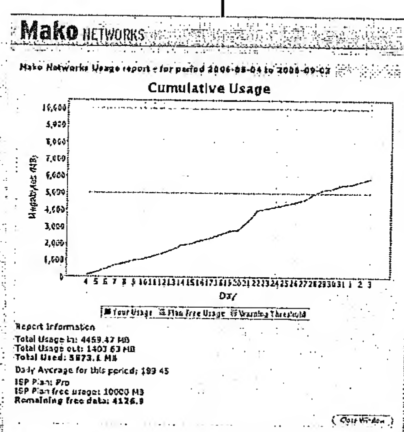
- Detailed, easy to understand reports to a PC level - including actual websites visited.
- Bill Shock protection with "Traffic Threshold" facility.
- Blocking of selected websites and categories to control Cyberslacking*.
- Ability to control network from any internet connected computer in the world.

Avoid being bitten by large Internet bills again with automatically generated warnings if you approach your broadband usage limit and AUTOMATIC pause in access when you hit your personalised maximum access.

See instantly and visually which PCs/users are clocking up your company's usage.

Drill down to actual sites visited in work time.





* Cyberslacking is the practice of employees using the Internet or other employer-provided resources for leisure during work hours contributing to inefficiencies up to 25%.

Mako
NETWORKS

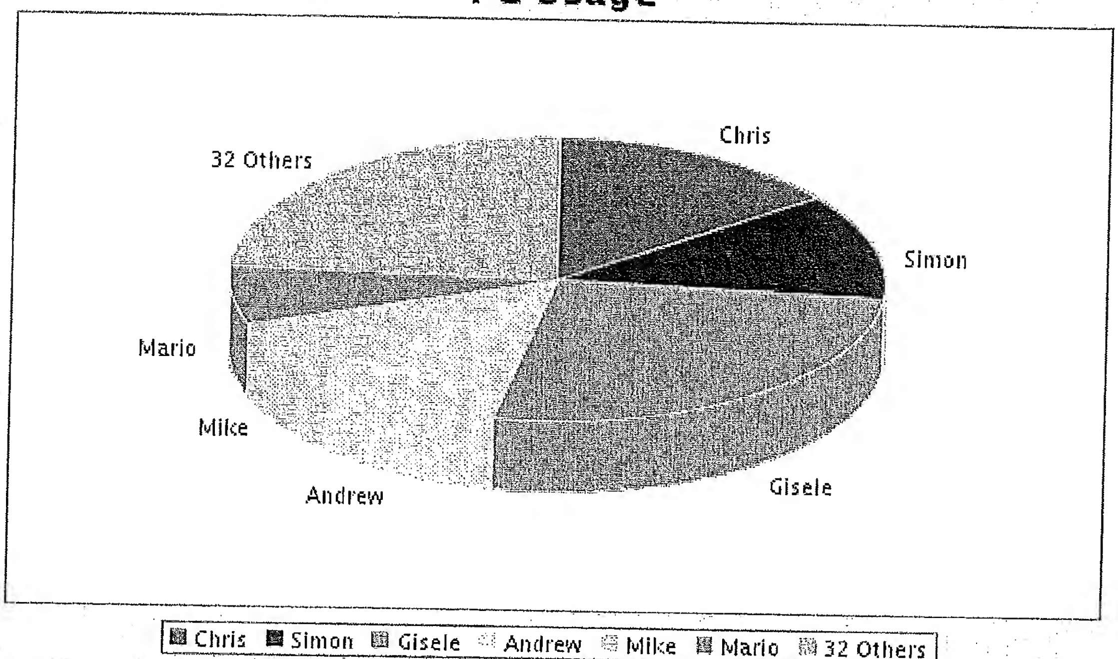
The Mako System

MANAGED NETWORKING AND SECURITY

Reports How Usage Is Generated

Mako Networks PC Usage Report
For period 2006-08-14 to 2006-09-13

PC Usage



Identification	Downloaded (MB)	Uploaded (MB)
Chris | edit	1,871.0463	104.1503
Simon | edit	1,308.0712	349.905
Gisele | edit	1,289.7882	2,317.7905
Andrew | edit	1,226.7675	48.651
Mike | edit	933.7928	47.2962
Mario | edit	856.9857	41.4792
Tom | edit	589.2465	7.4269
Eugen | edit	506.748	6.8151
Matt | edit	485.1812	17.441
Dennis G4 | edit	306.6743	14.3988

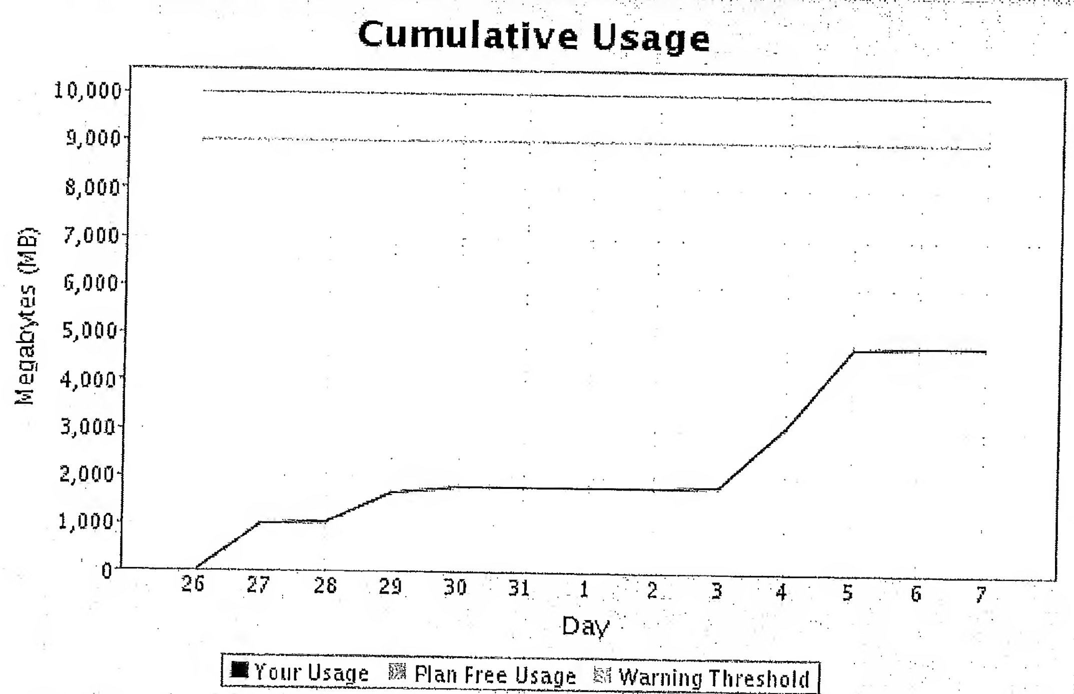
Mako
NETWORKS

The Mako System

MANAGED NETWORKING AND SECURITY

Reports on Total Usage

Mako Networks Usage report - for period 2006-08-26 to 2006-09-07



Report Information

Total Usage in: 3807.13 MB
Total Usage out: 994.23 MB
Total Used: 4801.36 MB

Daily Average for this period: 369.34

ISP Plan: Adventure
ISP Plan free usage: 10000 MB
Remaining free data: 5198.64

You have 19 days until the end of your billing cycle.
At your current average usage rate of 369.34 MB per day,
you will have used 11818.73 MB by the end of your cycle.

Close Window

Mako
NETWORKS ®

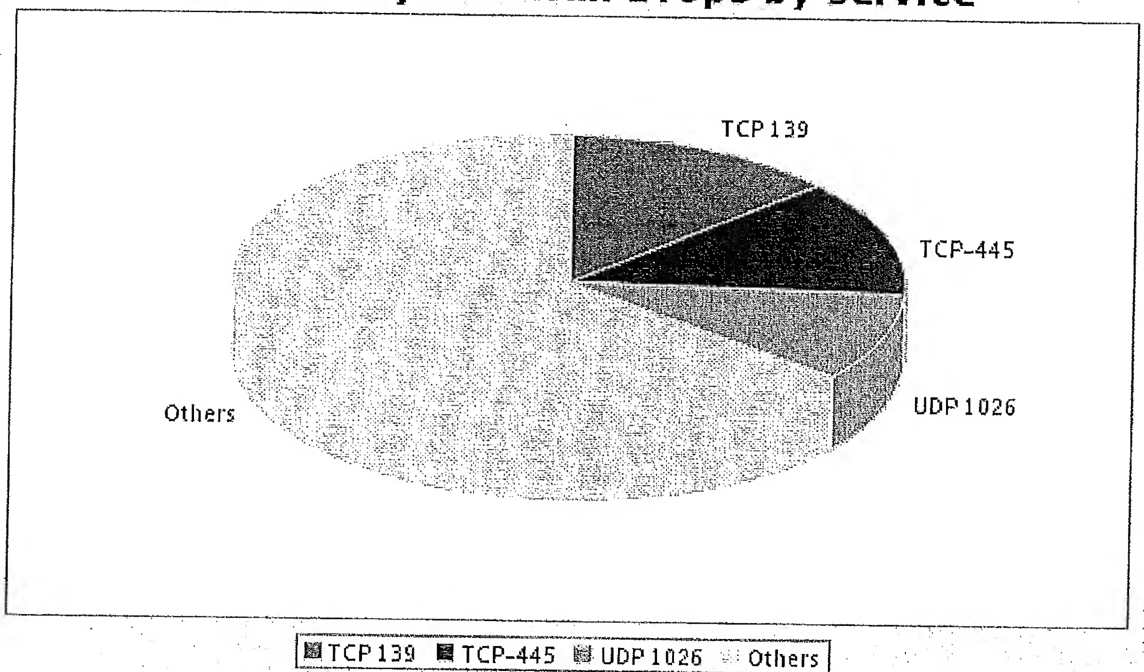
The Mako System

MANAGED NETWORKING AND SECURITY

Unwanted Intrusion Attempts

Mako Networks Firewall Usage Report
For period 2006-09-01 to 2006-09-14

Last 14 Days Firewall Drops by Service



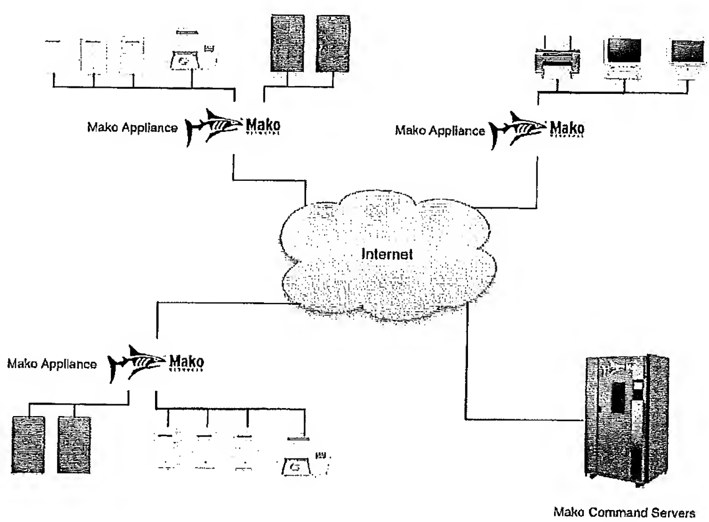
View the source of the blocked intrusions

Port/Type	Exploit Rating	Drops
139/TCP		1597
Microsoft Domain Service (UDP)		1552
Calender Access Protocol		1162
8/ICMP		564
TCP-500		423
Microsoft SQL Server		240
1027/UDP		232
Secure Shell		155

Mako
NETWORKS

Mako Networks System Summary

The Mako System is a complete departure from the traditional vendor model of hardware with optional management added. The award-winning, ISCA Certified Mako System is a combination of appliance and hosted central management platform that work together to provide a complete network connectivity and management solution designed specifically for SMEs. All configuration and appliance interaction takes place over authenticated https on the central management platform. No configuration takes place on the appliance. It is this operation as a System that drives all the commercial benefits for Mako customers.



The central management platform consists of web servers, application servers and databases protected by multiple firewalls and security systems. The bulk of the central management platform is made up of IBM hardware with a combination of proprietary Mako software running on a UNIX operating system. Mako's larger customers will typically install their own management platform for their customers that may or may not be part of Mako's global system. Mako Networks hosts its own globally shared central management platforms that are used mainly by the reseller channel and their customers. Mako end-user appliances are currently based on two hardware platforms (6086 and 7550) and offer the choice of multiple WAN interfaces including 3G, Ethernet and ADSL2+ across the range. A major feature of the solution is these appliances ship directly from manufacturing to warehouse to end-user without the need for on-box configuration. The appliances ship with patented proprietary software incorporating a default configuration enabling them to connect to the internet, communicate with the central command platform and retrieve their unique configuration.

This is the exhibit marked"SMG-2"
referred to in the affidavit of
Simon Mathew Gamble
sworn before me this 17/07/2009

Solicitor of the High Court of New Zealand

Once online, appliances regularly "check-in" with the command servers using a patented communication method. Unlike traditional vendor options, the Mako appliances initiate communication with the command servers negating the need for static IP addresses and individually pre-configured appliances. Every two minutes each appliance checks with the command platform if there is a need for configuration changes or firmware updates. The appliances also transmit their raw traffic logs to the servers for automatic interpretation and analysis.

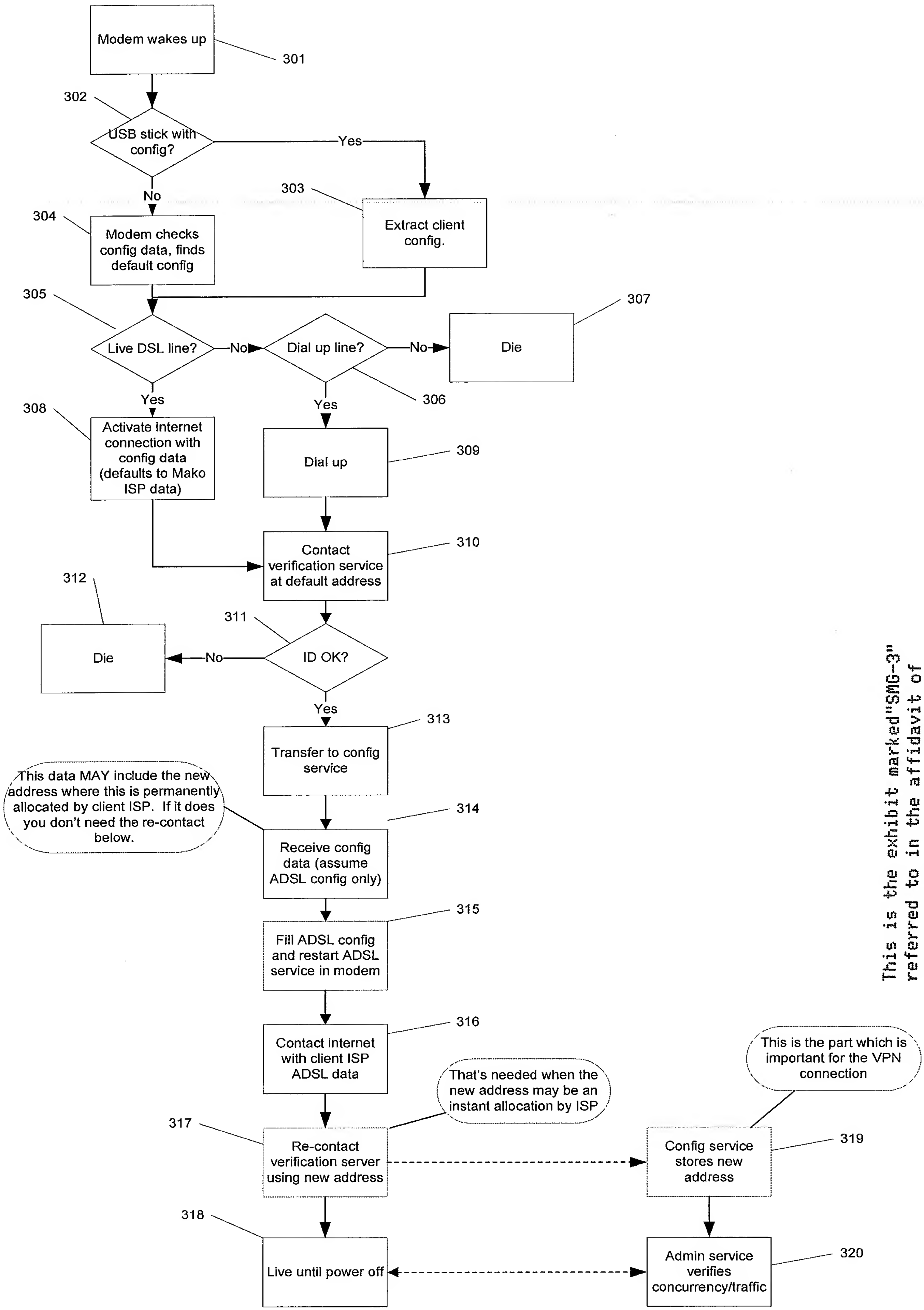
Because the command platform has automated responses to the interpreted data from the appliances, pro-active alerts are sent when necessary. Pro-active alerts include extraordinary usage, worm detection, intrusion detection and hardware triggers such as fan speed and CPU temperature. The command platform also sends monthly PDF reports on usage, intrusion attempts and even an easy to read company-wide summaries for end-users with more than one Mako-protected site.

The automated software and firmware upgrades mean that new services and increased functionality are added to the platform on an ongoing basis. This allows new chargeable services or free upgrades to be provided to the end-user ensuring the longest possible revenue cycle.

Help desk staff have access to the Diagnostics area on the command platform. Mako Diagnostics continues the Mako zero-touch philosophy giving support personnel the ability to remotely resolve network and connectivity issues without the need for onsite visits or technically competent end-users. With Mako Diagnostics help desks can receive real time feedback from Mako appliances simply by clicking buttons on the central management platform website. Diagnostics include; ADSL data, line noise, LAN connectivity, VPN connectivity, ARP lookups and ISP connection information. Mako Diagnostics reduce support costs and increase customer preference by empowering a help desk to very quickly identify and resolve problems.

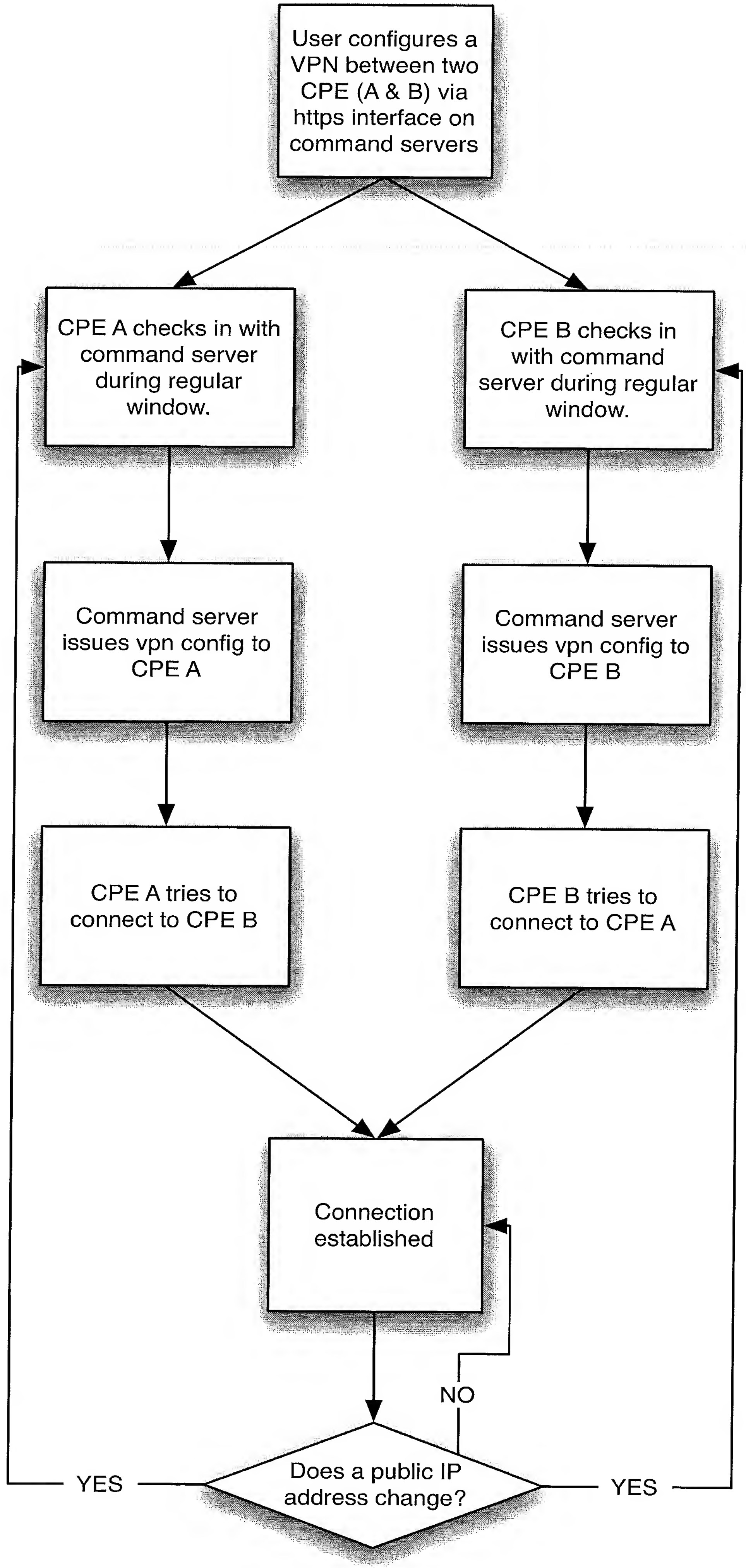
To summarise:

- Mako is a complete System not a range of standalone hardware with an added Management Platform
- The System provides a range of value added services to the end user
- The System is a combination of CPE and Management Servers
- All configurations takes place on the management servers via https
- Appliances require no direct configuration
- Mako has a philosophy of zero-touch appliances that begins with deployment
- The Mako System is pro-active with automated reports and alerts
- The Mako System is designed to be used by small to medium sized businesses and branch offices of larger organisations



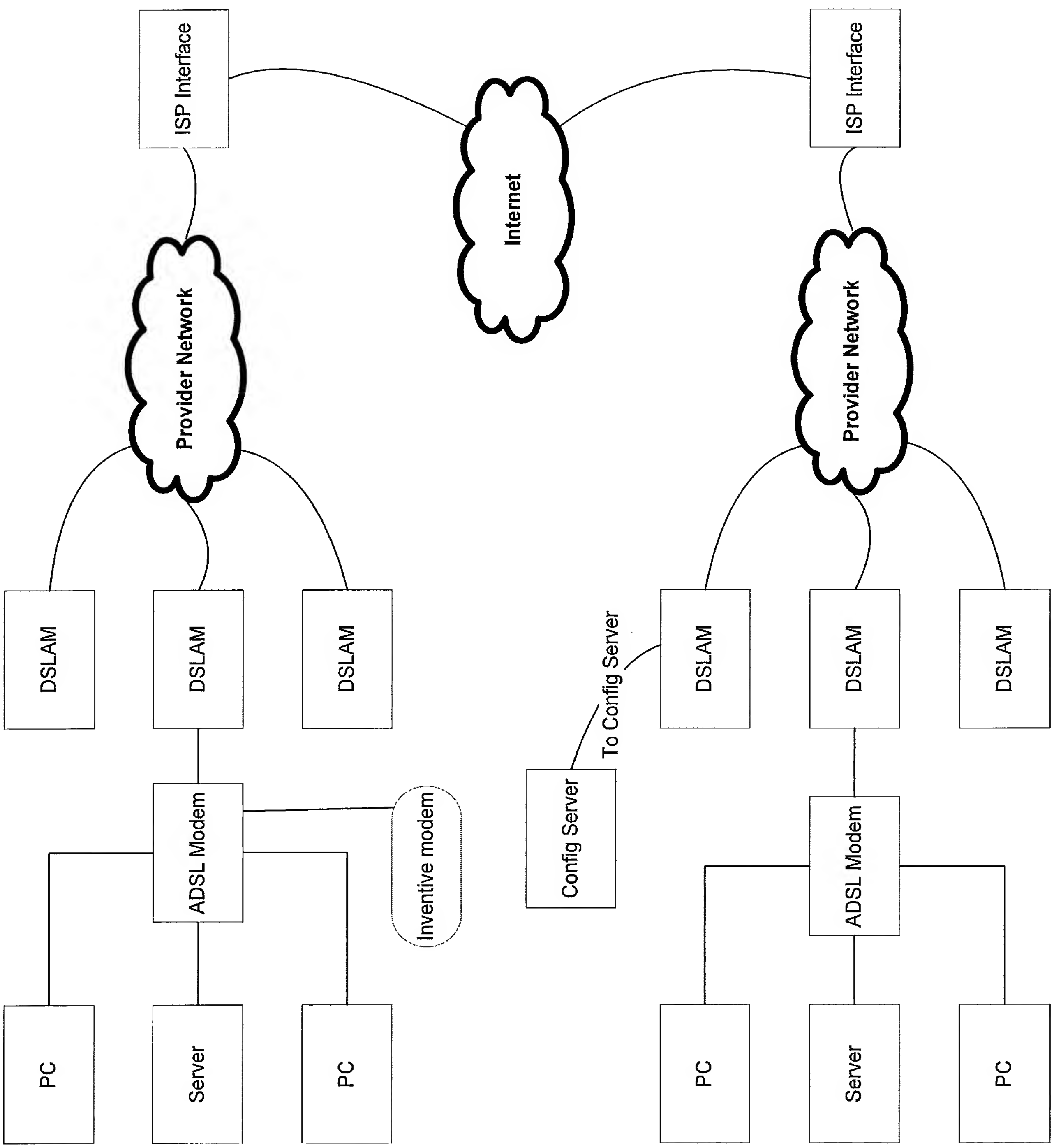
This is the exhibit marked "SMG-3" referred to in the affidavit of Simon Mathew Gamble sworn before me this 17/07/2009

Solicitor of the High Court of New Zealand



This is the exhibit marked "SMG-4" referred to in the affidavit of Simon Mathew Gamble sworn before me this 17/07/2009

Solicitor of the High Court of New Zealand



This is the exhibit marked"SMG-5"
referred to in the affidavit of
Simon Mathew Gamble
sworn before me this 17/07/2009

Solicitor of the High Court of New Zealand